GAMP 5 – A brief overview

IFF møde 2012-09-19

Conscience driven. Value adding

Kort fortalt

- NNIT er en af Danmarks fire største leverandører af it-services
- Fokusområder: It-rådgivning, udvikling,
  implementering og drift til life sciences, finans-
  sektoren, det offentlige og andre industrier
- Over 1.800 medarbejdere
- Omsætning i 2011: DKK 1,8 mia.
- Hovedkontor i Søborg
  - kontorer i seks lande: Schweiz, Tjekkiet, Kina, Filippinerne og USA
- Kunder i det meste af Europa
- Datterselskab af Novo Nordisk A/S

Agenda

- What is GAMP 5

- Key Concepts
- Life Cycle Approach
- Life Cycle Phases:
  - Concept
  - **Project**
  - Operation
  - Retirement
- Quality Risk Management
- Regulated Company Activities:
  - Governance for Achieving Compliance
  - System Specific Activities
- Supplier Activities

Background

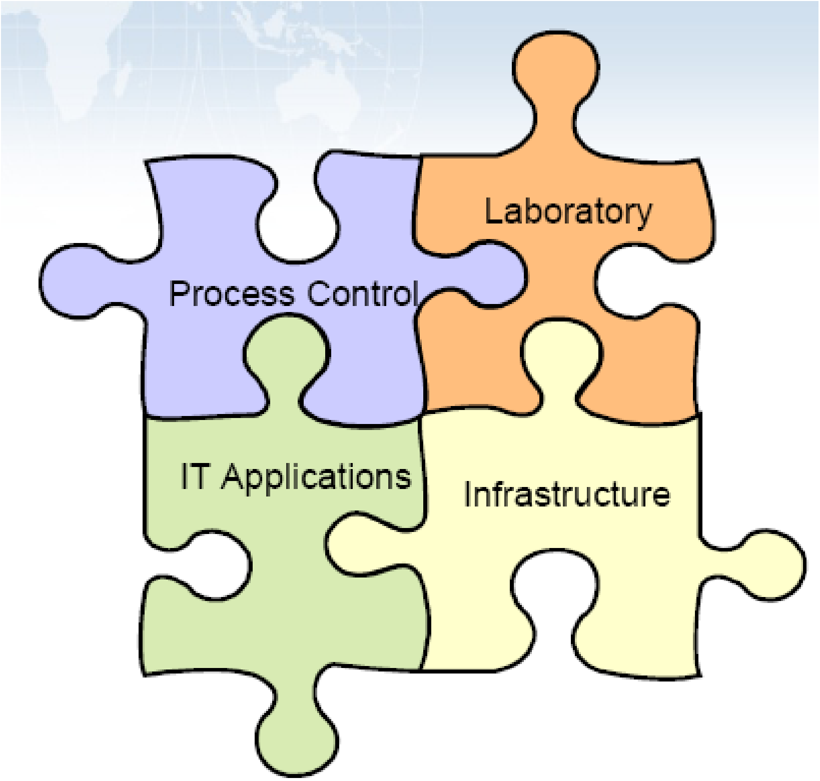
- Established in early 90’s
- More than **50 healthcare professionals**, from the Americas and Europe, participated in the production of GAMP 5 by contributing to groups producing new and revising existing material.

Core Purpose

- GAMP guidance aims to achieve computerized systems that **are fit for intended use** and **meet current regulatory requirements**, by building upon existing industry good practice in an efficient and effective manner.

The GAMP Guide

- The GAMP Guide contains the **validation framework** and associated procedures and guidelines. **It draws together the key principles and practices**, and describes how they can be applied to determine the extent and scope of validation for different types of systems, ensuring that validation is scaleable.



Practical Guidance

- Facilitates the **interpretation of regulatory requirements**
- Establishes a common language and terminology
- Promotes a **system life cycle approach** based on **good practice**
- Clarifies roles and responsibility
- *Not* a prescriptive method or a standard
  - but pragmatic guidance, approaches, and tools for the practitioner.
- *When* applied with expertise and good judgment:
  - offers a robust, cost effective approach.

Basic philosophy

- Focus attention on those **computerised systems** with most **impact on patient safety**, **product quality**, and **data integrity**

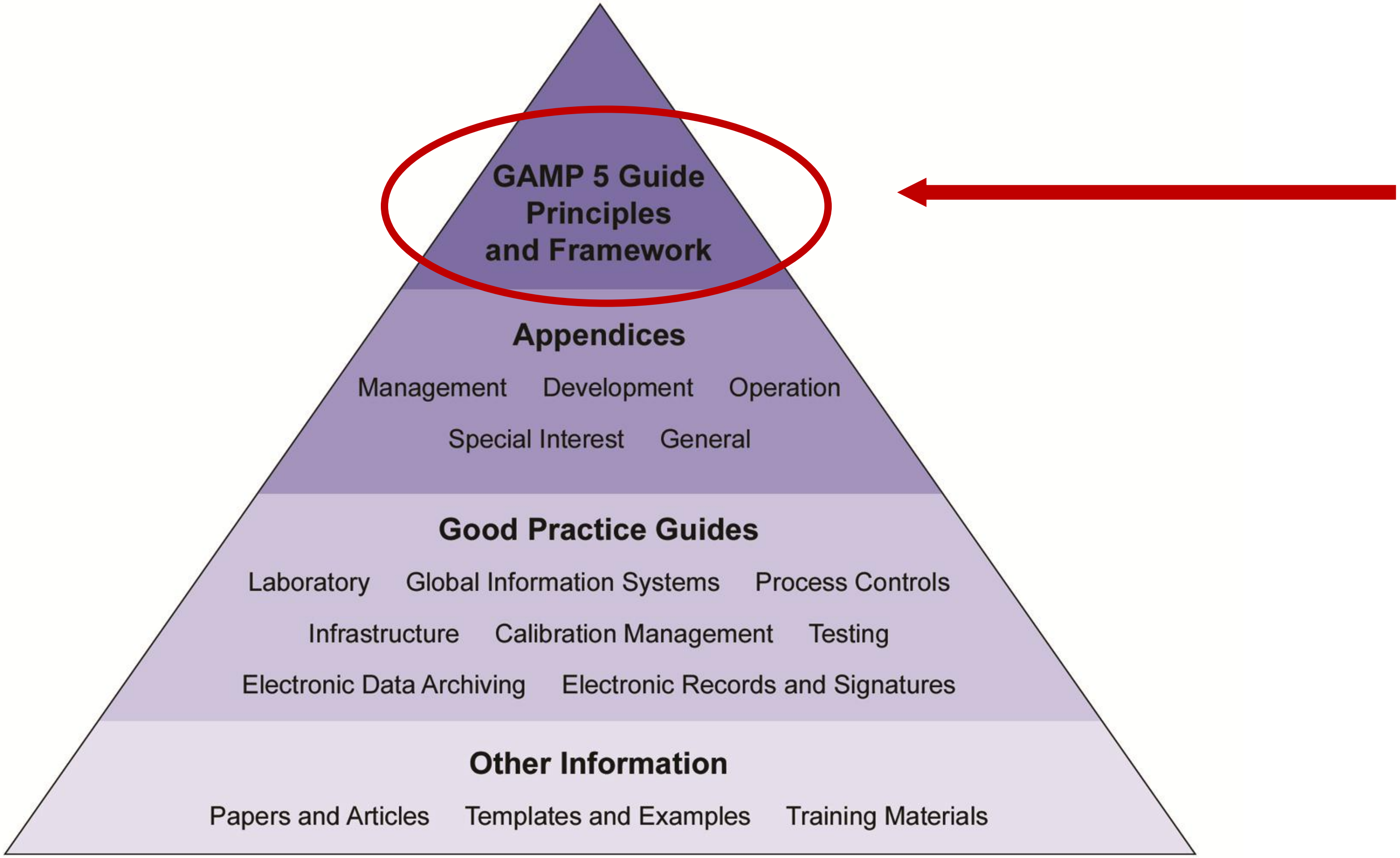
- **Avoid duplication of activities** (e.g. by fully integrating engineering and computer system activities so that they are only performed once)

- Leverage supplier activities to the maximum possible extent, while **still ensuring fitness for intended use**

Basic philosophy

- Scale all lifecycle activities and associated **documentation according to risk**, **complexity**, and novelty
- Recognise that most computerised systems are now based on **configurable packages**, many of them **networked**
- Acknowledge that traditional linear or waterfall development models are not the most appropriate in all cases

Structure of GAMP5



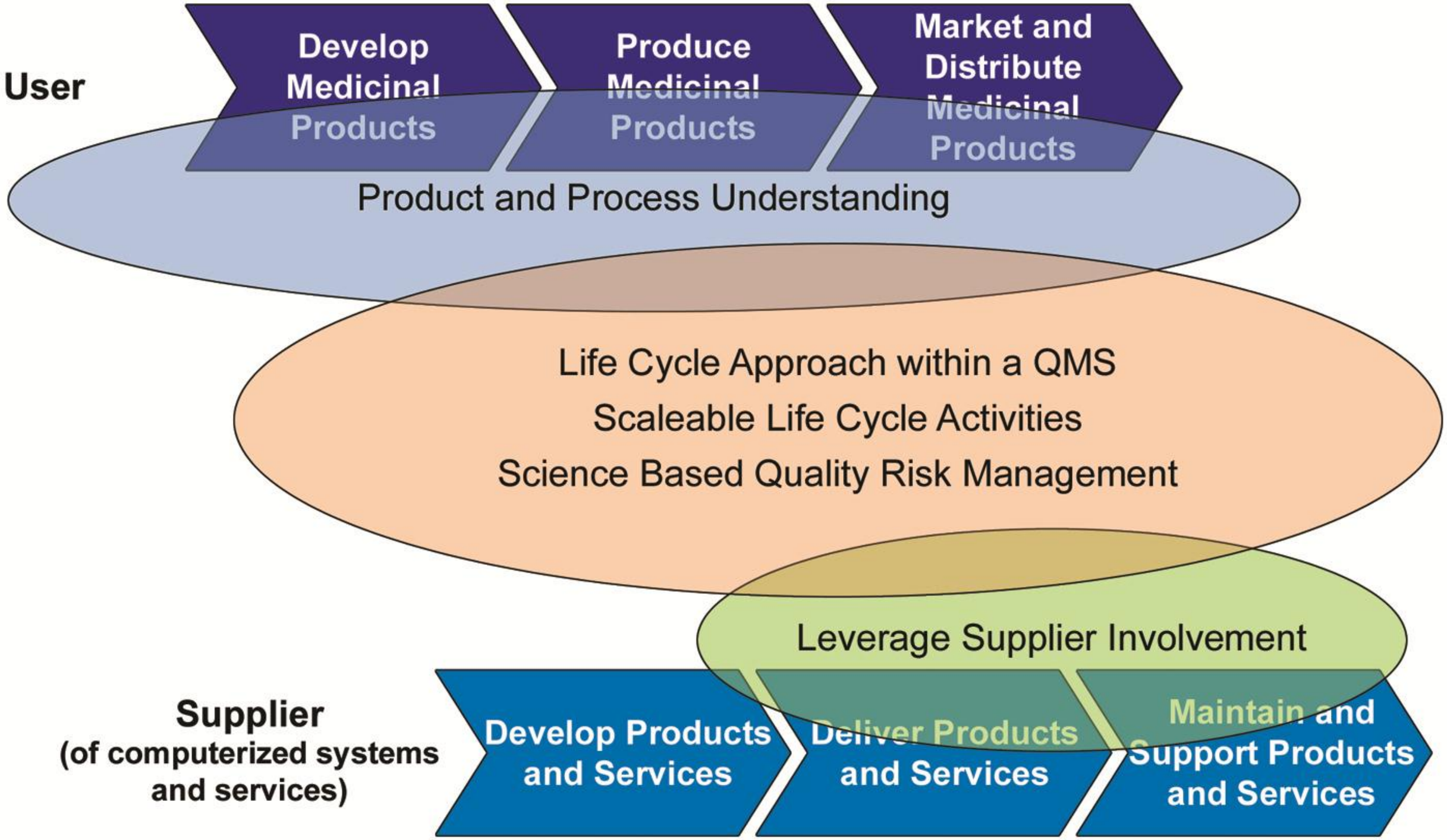
Source: Figure 1.2, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

The GAMP main body

The main body consist of:

- Key Concepts
- Life Cycle Approach
- Life Cycle Phases
- Quality Risk Management
- Regulated Company Activities
- Supplier Activities

Five Key Concepts


User
Develop Medicinal Products
Produce Medicinal Products
Market and Distribute Medicinal Products
Product and Process Understanding
Life Cycle Approach within a QMS
Scaleable Life Cycle Activities
Science Based Quality Risk Management
Leverage Supplier Involvement
Supplier (of computerized systems and services)
Develop Products and Services
Deliver Products and Services
Maintain and Support Products and Services

Source: Figure 2.1, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Life Cycle Approach Within a QMS

- Life cycle approach: **defining activities** in a systematic way from **understanding requirements to system retirement**
- Enables **management control** and a consistent approach across systems
- The life cycle should form an intrinsic part of the **company's Quality Management System (QMS)**
- The QMS should enable continuous process and system improvements based on **periodic review** and **evaluation, operational** and **performance data**, and **root-cause analysis of failures**
- Identified **improvements and corrective actions** should follow change management.

Product and Process Understanding

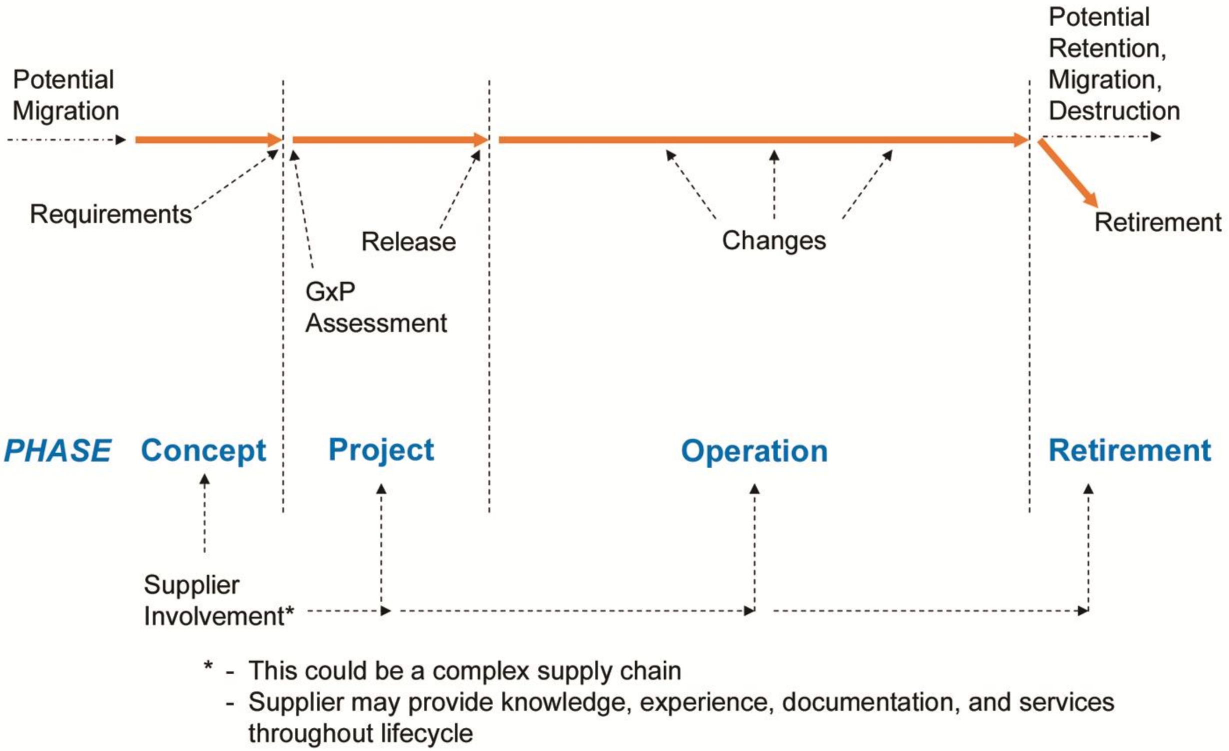
- An **understanding** of the supported **process is fundamental**
- Focus on risk to ***Patient Safety***, ***Product Quality***, and ***Data Integrity***
- Need to **understand risks** associated with a business process before the risks associated **with specific functions of computerized systems** can be assessed
- Specification of requirements should be focused on **critical aspects**
- The extent and detail of **requirement specification** should be based on the **associated risk**, **complexity**, and novelty of the system.

Leveraging Supplier Involvement

- Involvement could be:
  - Requirements gathering
  - Risk assessments
  - Creation of functional and other specifications
  - System configuration
  - Testing and other verification
  - Support and maintenance.
  - **Documentation should be assessed for suitability, accuracy and completeness**

Computer System Life Cycle

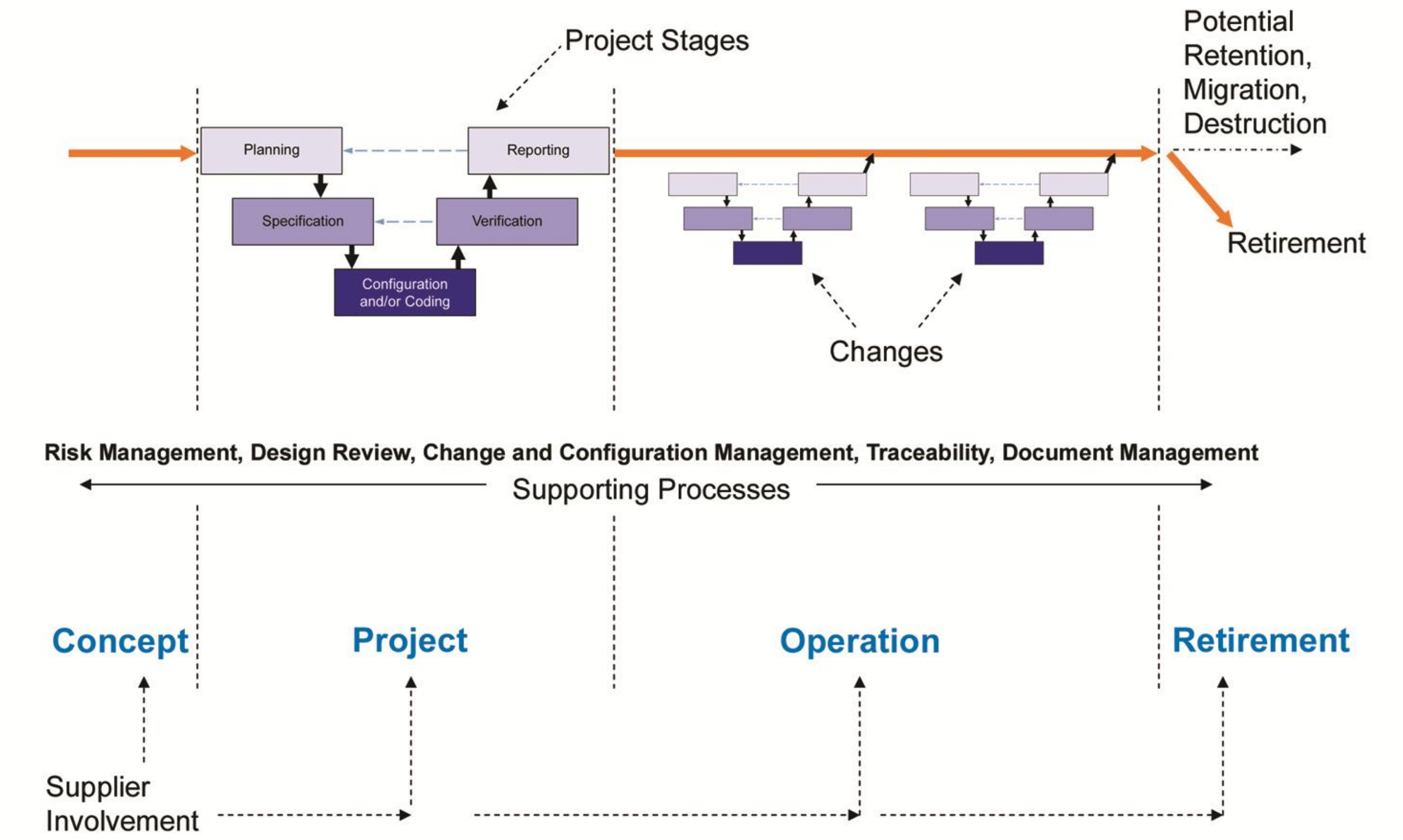
- The computerized system life cycle encompasses all activities **from initial concept to retirement** and **data migration or destruction**.



* - This could be a complex supply chain
- Supplier may provide knowledge, experience, documentation, and services throughout lifecycle

Source: Figure 3.2, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Specification and Verification



Source: Figure 4.1, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Planning

- Planning is an essential activity for any system development and should address all aspects including required activities, responsibilities, and timelines.
- Activities should be scaled according to:
  - System impact on patient safety, product quality and data integrity (risk assessment)
  - system complexity and novelty (architecture and categorization of system components)
  - Outcome of supplier assessment (supplier capability)
- **A clear understanding of requirements** is needed in order to facilitate effective planning. The development of requirements, therefore, is typically initiated during this phase.

Specification, Configuration and Coding

- Functional and design specifications may be the responsibility of the supplier, but the user needs to ensure that they are adequate to build a reliable and robust system.
  - Specifications should be managed under change control.

- Specification activities may be distinct or tightly coupled with configuration and coding activities depending on the software development method being adopted.

- **The system should be configured in accordance with a controlled and repeatable process**.

- Any software coding required should be carried out in accordance with defined standards and be subject to review.

- **Configuration management is an intrinsic and vital aspect of controlled configuration and coding**.

Verification

- Testing of computerized systems is a combination of:
  - Testing conducted by the Supplier during the System Product Life Cycle
  - Testing conducted by the Supplier (or integrator) during application specific development or configuration
  - Testing conducted by Regulated Company

- This is a key area for leveraging supplier activity
  - **How much** of the testing conducted by the **Supplier can be leveraged**?
  - **What testing** has to be conducted by the **Regulated Company**?

Verification (D5)

- User Testing Activities
  - power failure testing especially
    - prevention against loss of critical data or loss of control action
    - ease of controlled restart.
  - system access and security features.
  - audit trails and logging of critical actions including manual interactions.
  - manual data entry features, input validation.
  - electronic signature features.
  - alarms and error messages

Verification (D5)

- User Testing Activities
  - critical calculations.
  - critical transactions.
  - transfer of critical data into other packages or systems for further processing
  - Interfaces and data transfers.
  - backup and restore.
  - data archival and retrieval.
  - ability to deal with high volume loads

Verification - Supplier

- Don’t forget the test environment
  - Should be **comparable** to the regulated company's **production environment**
    - Differences must be documented
      - Assessed for level of impact
    - Differences may lead to the need for **additional testing** by the regulated company
  - Must be **maintained under change control**
  - Documentation and control must support reconstruction or emulation

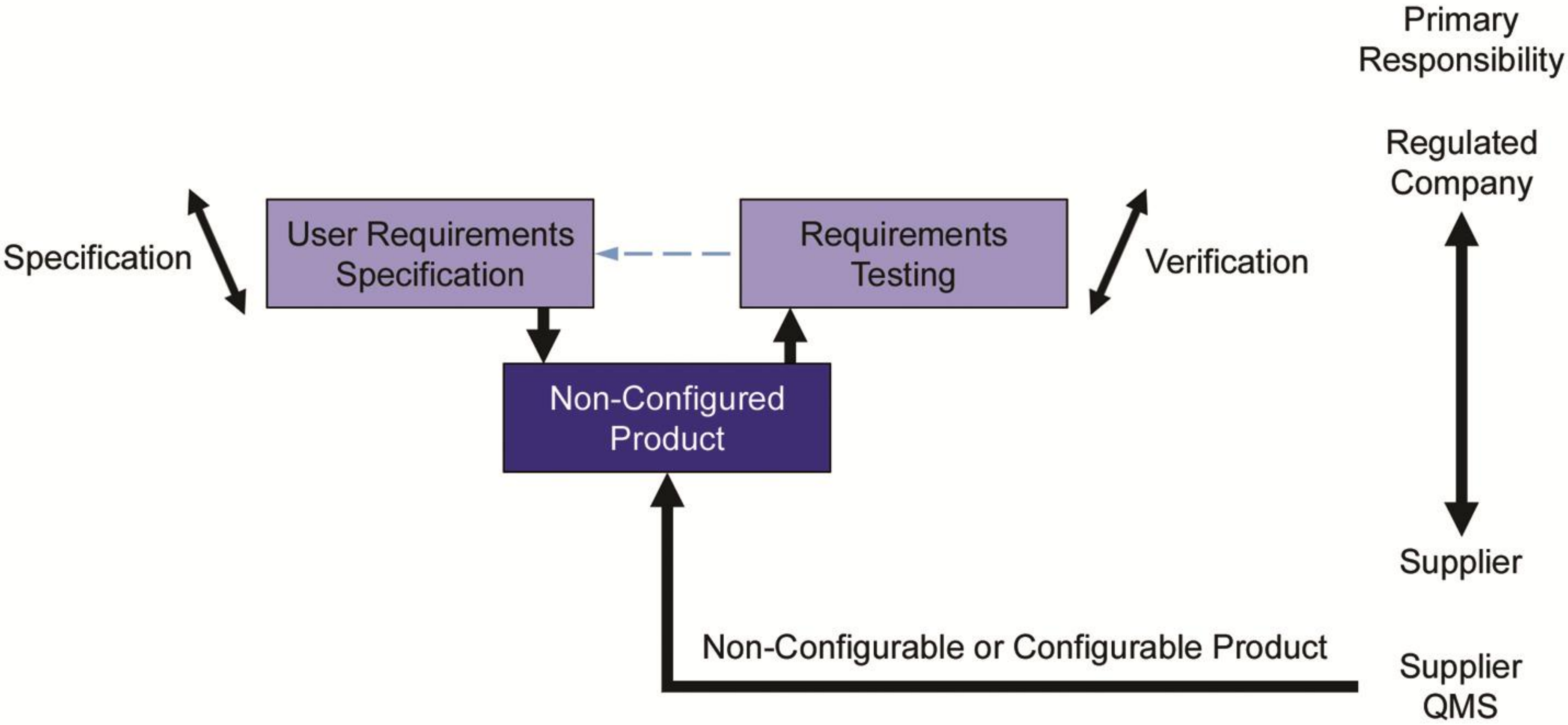
Categories of software (M4)
Category 1: Infrastructure Software

- There are two principle types of software in this category.
  - **Established commercially available layered software**: Applications are developed to run under the control of this kind of software. This includes operating systems, database managers, programming languages, middleware, ladder logic interpreters, statistical programming tools like SAS® , and spreadsheet software (applications like Microsoft Excel® or Lotus 1-2-3® , not spreadsheets developed for business purposes).
  - **Infrastructure software tools**: This includes such tools as network monitoring software, batch scheduling tools, and configuration management tools. However, risk assessment should be carried out on tools with potential high impact, such as for password management or security management, to determine whether additional controls are appropriate.

Categories of software (M4)
Category 3: Non-Configured Software

- This category includes **<u>“off-the-shelf” applications used for business purposes</u>**. It includes both systems that cannot be configured to conform to business processes (although configuration of run-time parameters is permitted) and systems that are configurable but for which only the default configuration is used.

- Standard Software Packages!!

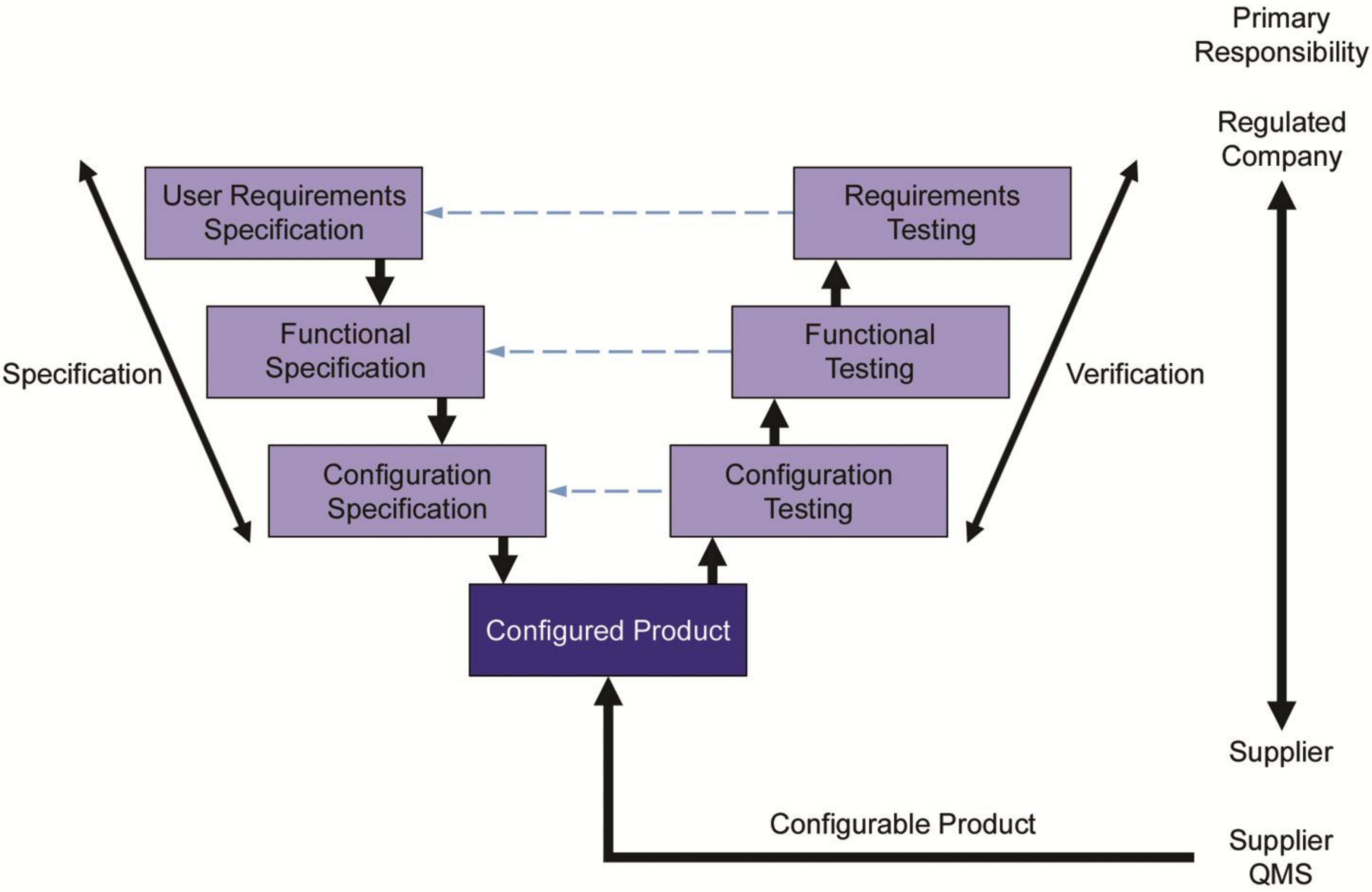


Source: Figure 4.2, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Categories of software (M4)

Category 4: Configured Software Packages

- Configurable software packages provide standard interfaces and functions that enable configuration of user specific business processes. **This involves configuring predefined software modules**.



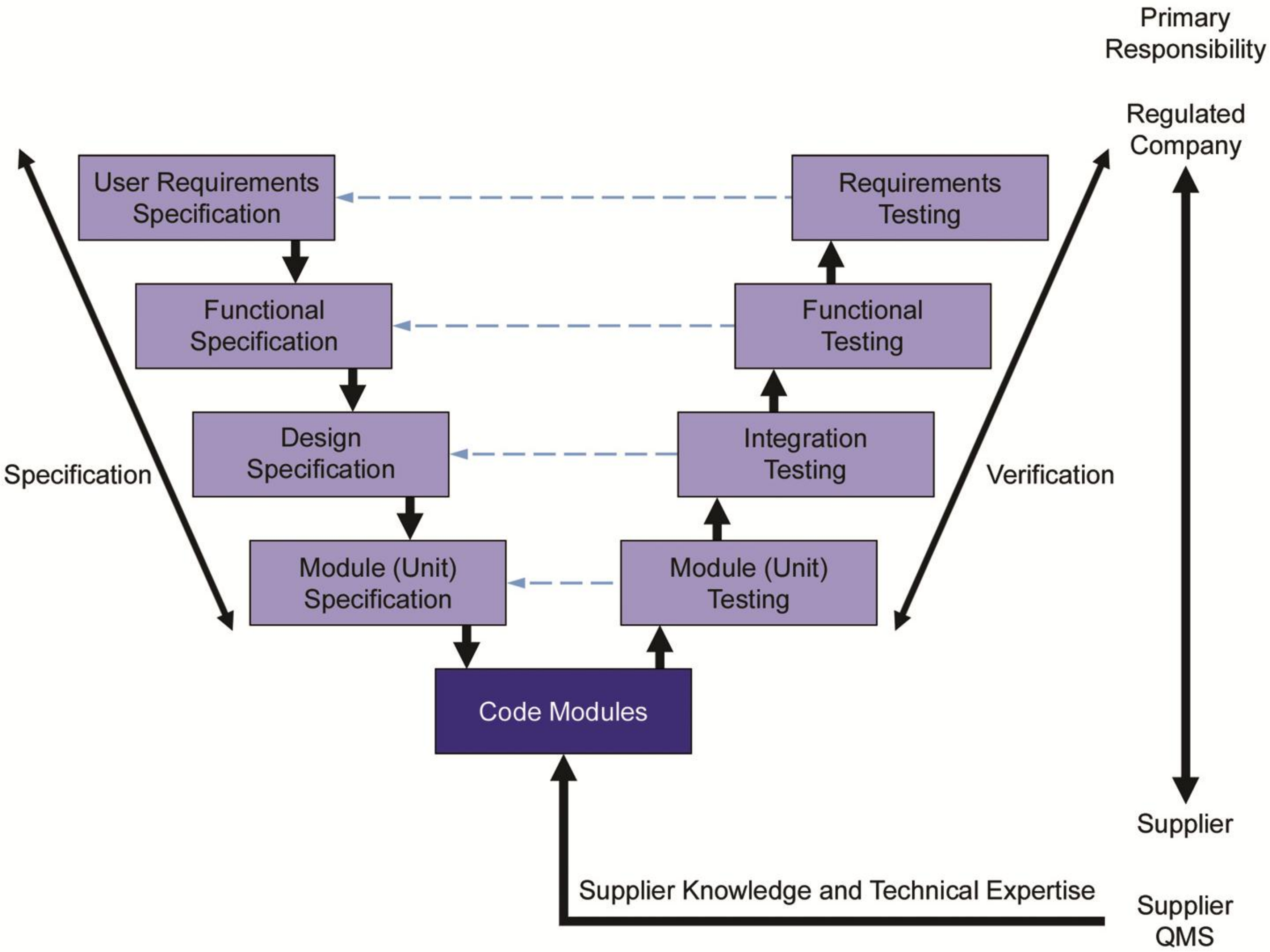
Source: Figure 4.3, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Categories of software (M4)

Category 5: Custom (Bespoke) Software

- These systems or subsystems are developed to meet the specific needs of the regulated company.

Nice, Promenade des Anglais - Patrick Murris, juillet 2004 - www.alpix.com/nice



Primary Responsibility

Regulated Company

User Requirements Specification

Requirements Testing

Functional Specification

Functional Testing

Design Specification

Integration Testing

Specification

Verification

Module (Unit) Specification

Module (Unit) Testing

Code Modules

Supplier

Supplier Knowledge and Technical Expertise

Supplier QMS

Source: Figure 4.4, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Quality Risk Management

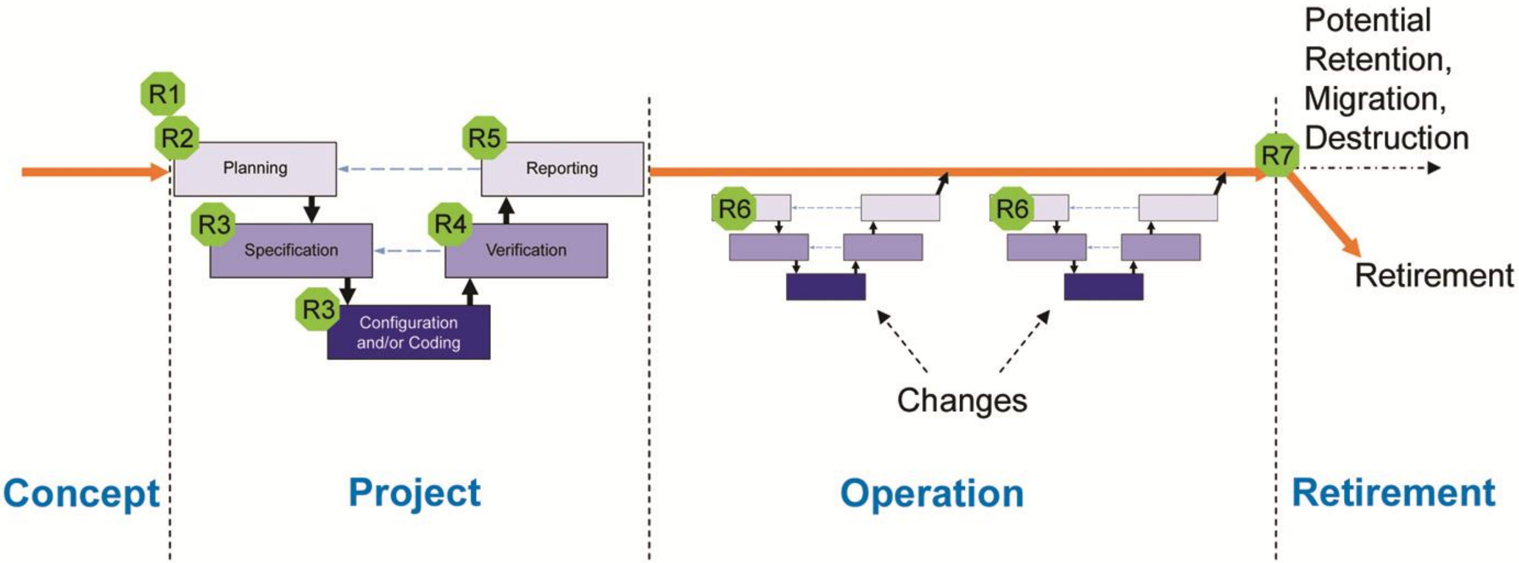
Section 5 (M3)

Quality Risk Management

- Quality risk management is a systematic process for the assessment, control, communication, and review of risks

- An **iterative process** used throughout the entire computerized system **life cycle from concept to retirement**

The Life Cycle Phases and Risk Assessment



R1 Initial risk assessment

R2 Risk-based decisions during planning

R3 Functional risk assessments

R4 Risk-based decisions during test planning

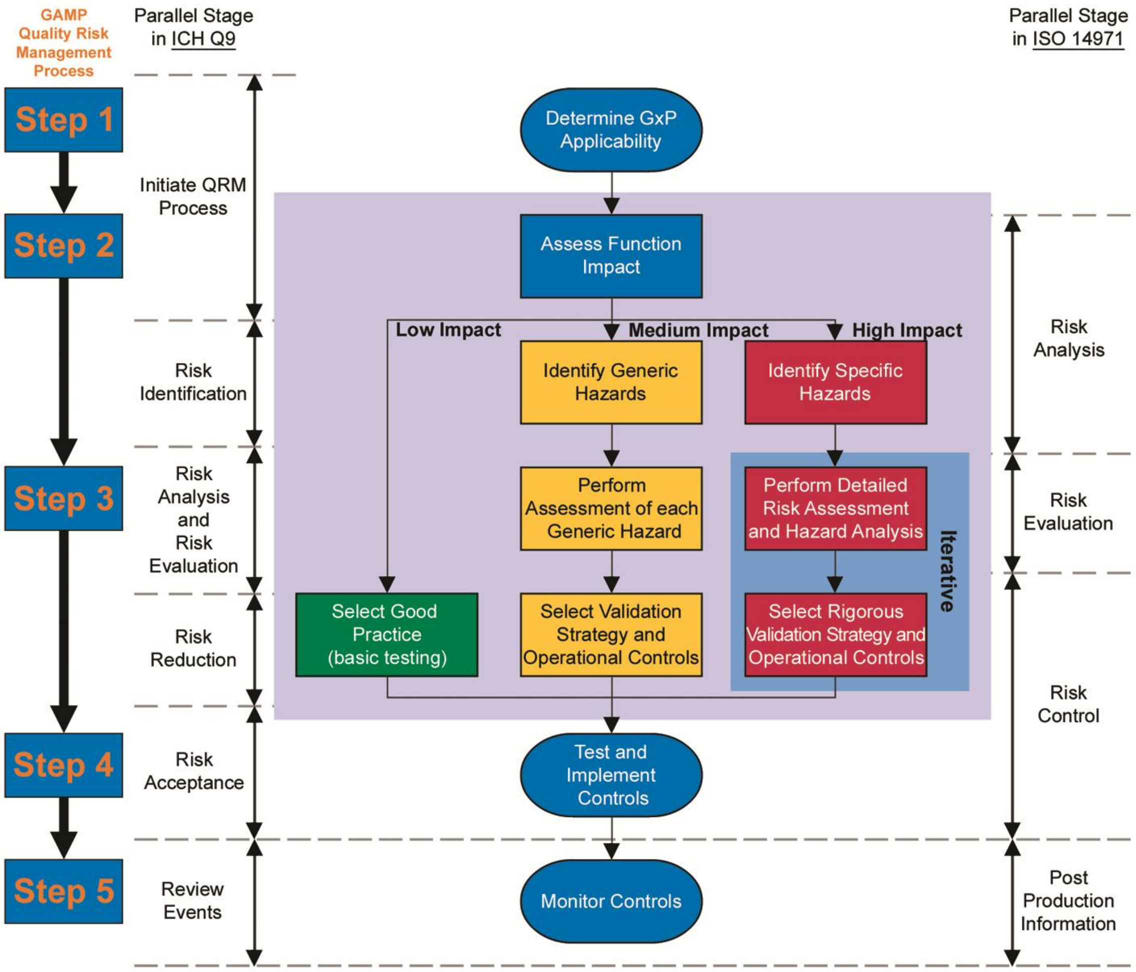
R5 Risk-based decisions during planning of operational activities

R6 Functional risk assessments in change control

R7 Risk-based decisions when planning system retirement

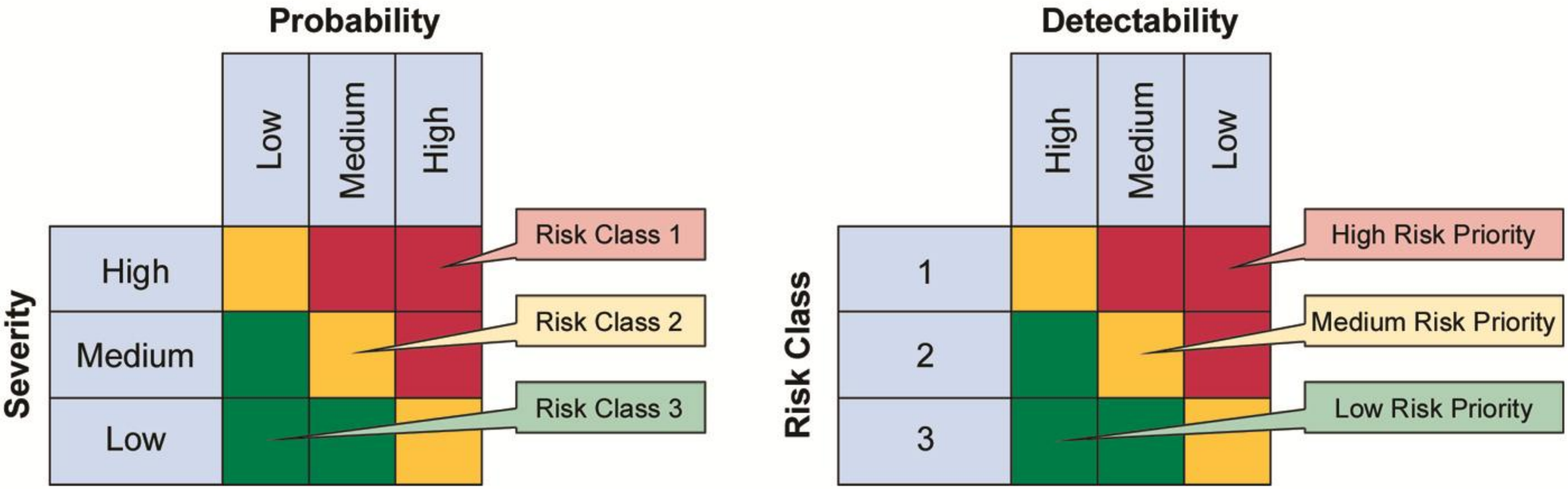
Source: Figure M3.3, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Different standards


GAMP Quality Risk Management Process
Parallel Stage in ICH Q9
Parallel Stage in ISO 14971
Step 1
Step 2
Step 3
Step 4
Step 5
Initiate QRM Process
Risk Identification
Risk Analysis and Risk Evaluation
Risk Reduction
Risk Acceptance
Review Events
Determine GxP Applicability
Assess Function Impact
Low Impact
Medium Impact
High Impact
Identify Generic Hazards
Identify Specific Hazards
Perform Assessment of each Generic Hazard
Perform Detailed Risk Assessment and Hazard Analysis
Iterative
Select Good Practice (basic testing)
Select Validation Strategy and Operational Controls
Select Rigorous Validation Strategy and Operational Controls
Test and Implement Controls
Monitor Controls
Risk Analysis
Risk Evaluation
Risk Control
Post Production Information

Source: Figure M3.10, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Method



Severity	Probability: Low	Probability: Medium	Probability: High
High	🟨	🟥	🟥
Medium	🟩	🟨	🟥
Low	🟩	🟩	🟨

🟥 Risk Class 1
🟨 Risk Class 2
🟩 Risk Class 3

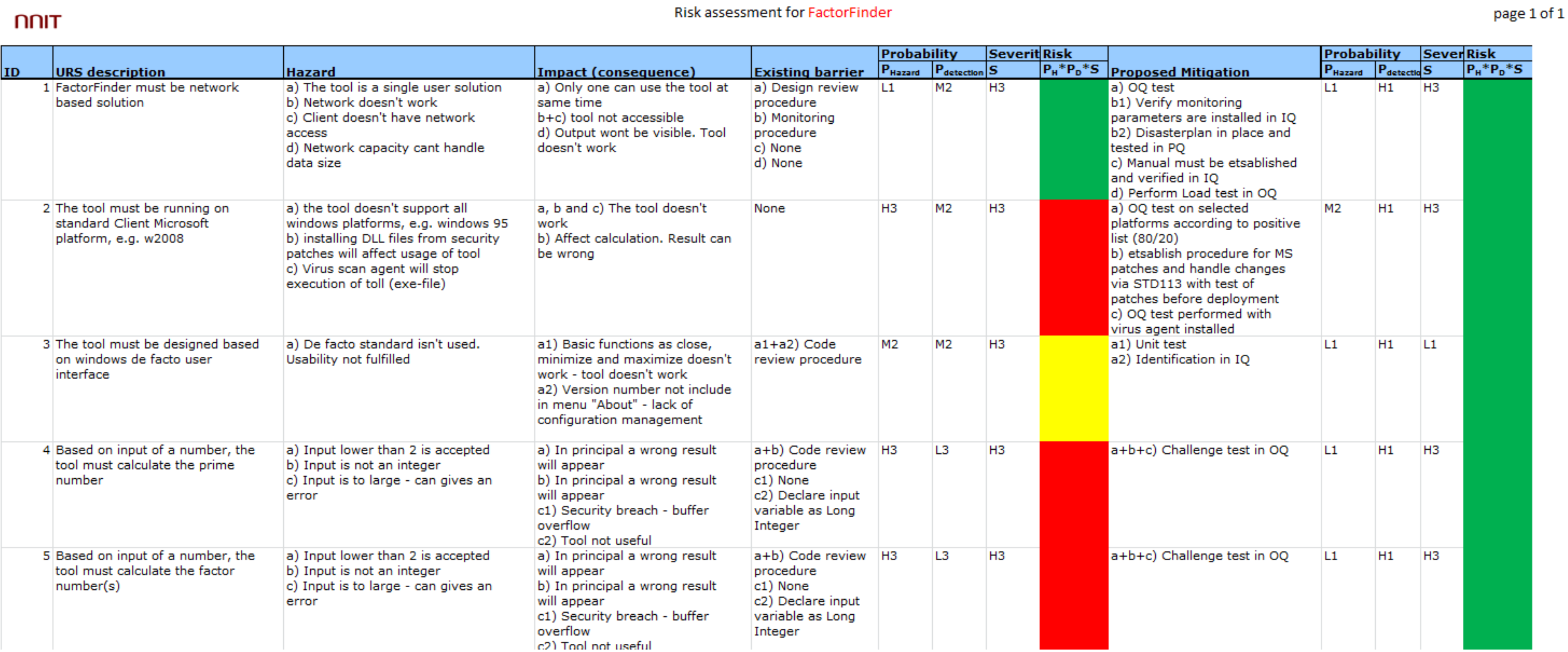
Risk Class	Detectability: High	Detectability: Medium	Detectability: Low
1	🟨	🟥	🟥
2	🟩	🟨	🟥
3	🟩	🟩	🟨

🟥 High Risk Priority
🟨 Medium Risk Priority
🟩 Low Risk Priority

Severity = Impact on Patient Safety, Product Quality, and Data Integrity (or other harm)
Probability = Likelihood of the fault occuring
Risk Class = Severity × Probability

Detectability = Likelihood that the fault will be noted before harm occurs
Risk Priority = Risk Class × Detectability

Source: Figure M3.5, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.



nnit

Risk assessment for FactorFinder

page 1 of 1

ID	URS description	Hazard	Impact (consequence)	Existing barrier	Probability		Severit	Risk	Proposed Mitigation	Probability		Sever	Risk
					P_{Hazard}	$P_{detection}$	S	P_H*P_D*S		P_{Hazard}	$P_{detectio}$	S	P_H*P_D*S
1	FactorFinder must be network based solution	a) The tool is a single user solution b) Network doesn't work c) Client doesn't have network access d) Network capacity cant handle data size	a) Only one can use the tool at same time b+c) tool not accessible d) Output wont be visible. Tool doesn't work	a) Design review procedure b) Monitoring procedure c) None d) None	L1	M2	H3	🟩	a) OQ test b1) Verify monitoring parameters are installed in IQ b2) Disasterplan in place and tested in PQ c) Manual must be etsablished and verified in IQ d) Perform Load test in OQ	L1	H1	H3	🟩
2	The tool must be running on standard Client Microsoft platform, e.g. w2008	a) the tool doesn't support all windows platforms, e.g. windows 95 b) installing DLL files from security patches will affect usage of tool c) Virus scan agent will stop execution of toll (exe-file)	a, b and c) The tool doesn't work b) Affect calculation. Result can be wrong	None	H3	M2	H3	🟥	a) OQ test on selected platforms according to positive list (80/20) b) etsablish procedure for MS patches and handle changes via STD113 with test of patches before deployment c) OQ test performed with virus agent installed	M2	H1	H3	🟩
3	The tool must be designed based on windows de facto user interface	a) De facto standard isn't used. Usability not fulfilled	a1) Basic functions as close, minimize and maximize doesn't work - tool doesn't work a2) Version number not include in menu "About" - lack of configuration management	a1+a2) Code review procedure	M2	M2	H3	🟨	a1) Unit test a2) Identification in IQ	L1	H1	L1	🟩
4	Based on input of a number, the tool must calculate the prime number	a) Input lower than 2 is accepted b) Input is not an integer c) Input is to large - can gives an error	a) In principal a wrong result will appear b) In principal a wrong result will appear c1) Security breach - buffer overflow c2) Tool not useful	a+b) Code review procedure c1) None c2) Declare input variable as Long Integer	H3	L3	H3	🟥	a+b+c) Challenge test in OQ	L1	H1	H3	🟩
5	Based on input of a number, the tool must calculate the factor number(s)	a) Input lower than 2 is accepted b) Input is not an integer c) Input is to large - can gives an error	a) In principal a wrong result will appear b) In principal a wrong result will appear c1) Security breach - buffer overflow c2) Tool not useful	a+b) Code review procedure c1) None c2) Declare input variable as Long Integer	H3	L3	H3	🟥	a+b+c) Challenge test in OQ	L1	H1	H3	🟩

Regulated Company Activities

Section 6

Why Governance?

- To ensure **compliance**
- To ensure **fitness for intended use**
- Achieving robust, cost effective, compliance requires strong governance
- The activities require a **defined** organizational and governance framework
- **Governance is the responsibility of the regulated company**

Governance & Organisational Management

- Identify and comply with GxP requirements
- **<u>Integrate life cycle activities into quality management system</u>**
- **<u>Identify and assess each system</u>**
- Ensure systems compliant and fit for use according to SOPs
- Follow a validation framework, validation plans and reports
- Maintain compliance throughout the lifetime of a system

System Activities for Effective Governance

- Maintaining the system inventory
- Impact of systems on patient safety, product quality, data integrity
- Defined roles and responsibilities
- Defining the computerized system life cycle approach

System Activities for Effective Governance

- Life cycle planning, supplier assessment, risk management, specification, verification, reporting activities and documents

- System operation and management, operating procedures for end users and administrators

- Record and data management

- Security management

Product and Process Understanding

- An understanding of the supported process is fundamental:
  - For determining **system requirements**
  - As a basis for making **science and risk based decisions** to assure that the **system is designed** and verified to be **fit for its intended use**.

NNIT
Conscience driven. Value adding

Reg. Company Activities for a System

- Identify
  - the compliance standards
  - the system
  - key individuals
- Develop
  - The URS
- The strategy for achieving compliance
  - Risk assessment
  - Assessment of system components
  - Supplier assessment
- Plan
- Review and approve key specifications
- Develop test strategy
- Test
- Report & release
- Maintain system compliance during operation
- System retirement

Regulated Company Management

- Set up the Governance Structure
- Ensure funding for Governance
- Ensure policies and procedures available
- Appoint Process Owner
- Appoint System Owner
- Appoint Project Manager
- Ensure appropriate SME’s available
- Define role of Quality Unit

Supplier Activities

Section 7

Suppliers Role

- Suppliers (including internal suppliers) play an important support role in achieving and maintaining system compliance and fitness for intended use
- May be key SME’s
- Provide key documentation
- Performing testing
- Providing support e.g. change control

What do we want from suppliers?

- Stable systems designed and developed using Good Practice:
  - Establish QMS
  - Establish requirements
  - Quality planning
  - Assessments of sub-suppliers
  - Produce specifications
  - Perform design review
  - Software production/ configuration
  - Perform testing
  - Commercial release of system
  - Provide user documentation and training
  - Support and maintain the system in operations
  - System replacement and retirement

Planning requests from Regulated Company

- If you want the supplier to deliver
  - Delivery must be identified and described
  - A common target must be established

Planning: Which QMS?

- If you want the supplier to follow your policies, procedures and standards
  - This must be made clear in the RFP (external supplier) and project documentation
  - Documentation must be provided
  - Supplier personnel must be trained before work starts
  - Compliance must be assured
    - Quality Plan

- If **you use the supplier's policies, procedures and standards**
  - The supplier's practices must be assessed for suitability, accuracy and completeness
  - Compliance must be assured throughout the life cycle
    - Quality Plan
    - Supplier assessment
  - Supplier assessment is important

Planning answers from Supplier

- Quality Plan and /or Statement of Work must define
  - Application of QMS
  - Roles and responsibilities for:
    - Regulated Company
    - Supplier
  - Lifecycle activities
    - Deliverables
  - Supporting Activities
    - Training
    - Change management
    - Reviews
    - Documentation
    - Approvals

Supplier QA

- Supplier QA – role and responsibility
  - Ensuring application of supplier QMS
  - Depends on what is being provided and risk
  - Eg. Appropriate levels of :
    - Software management
    - Document management
    - Configuration control
    - Change control

Summary

- I have presented GAMP5
  - The structure
  - Key concepts
  - Life cycle approach
  - Quality risk management
  - Regulated company activities
  - Supplier activities

- Take a look at the document and the other Good Practice Guides
- Use extracts as feasible